ABSTRACT

A method for use by a telecommunication terminal (10) in checking whether a candidate RAND in an EAP/SIM RAND challenge is likely a replay, based on using a Bloom filter including a vector data structure (21) for determining (admittedly sometimes erroneously) whether the candidate RAND is in a set of previously used RAND values. The components of the vector data structure (21) are set to one or left at zero depending on whether pointers corresponding to the previously used RAND values point to them. The pointers can be hash functions or can be constructed from the previously used RAND values. To provide for smooth filter performance at points in time when the Bloom filter is full and cannot hold information for any new previously used RAND values, the vector data structure (21) is partitioned into more than one part, and only one part is reset and re-initialized at a time.